

Notice of Allowability

Application No.

09/976,050

Examiner

Thomas M. Ho

Applicant(s)

NISHIMURA, SAORI

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 11/08/05.
2. ☒ The allowed claim(s) is/are 2,4-6 and 10.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINERS AMENDMENT

1. Claims 2, 4-6, 10 are pending.

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Chtistophe F.lair, Reg. No. 54248 at (703)770-7797 on 2/6/06.

Claims 6 and 10 recite: "transmitted form the terminal unit" which for purposes of examination has been amended to recite "transmitted from the terminal unit". In claim 6, this is present in the fourth step, while in claim 10, it present in the "first key encoding means"

Reasons for Allowance

In reference to claim 2:

Mooney et al. (Column 11, lines 1-35) discloses an IC card terminal unit comprising:

- Communication means for communicating data between two IC cards, where the communication means is the “remote key transfer method” which is comprised of a network. (Column 11, lines 25-30)
- First key setting means for storing a second key for encoding or decoding a first key in the two IC cards respectively by transmitting a key setting instruction to which the second key is added to the two IC cards through the communication means, where the encoding or decoding of the first key(the key within the smartcard) is performed with a second key, the encryption key which is converted from an authentication question. (Column 11, lines 20-25)
- Key generation means for generating the first key for encoding or decoding data in the former IC card by transmitting a key generation instruction to one of the two IC cards, where the key generation means is the ability of the owner to generate a key (Column 10, lines 62-67) which is used for encoding data between two parties. (Column 11, lines 35-40)
- Key takeout means for taking out the first key generated in the former IC card generating the first key by the key generation means through the communication means by transmitting a key takeout instruction to the former IC card through the communication means, where the key takeout means is the means for reading the key from the owner IC card through the smartcard reader, and the instruction for transmitting a takeout instruction is a request to export to the key. (Column 11, lines 1-35)

Mooney et al. fails to explicitly disclose:

Confirmation means for confirming whether setting of the second key by the first key setting means normally ends.

The Examiner takes official notice that confirmation means for confirming whether an operation of a digital system was successfully completely was well known at the time of invention.

For Example, computer systems that use access messages such as “access denied” or “access granted”, or “general protection fault” or “operation successful” or “save completed” or “format completed” are all confirmation means to indicated whether a given operation on a computer was successfully completed.

Furthermore, Mooney et al. (Column 14, lines 8-15) states that the smart card used within is compatible with smartcard industry standard ISO 7816. ISO 7816-3, pages 17-18 “section 3.5.b Structure and processing of commands” indicates that a value bit to return values indicating whether or not a file transfer is successful or whether an instruction to a smartcard “properly ends”

Mooney et al. (Column 14, lines 8-15) further states that “One skilled in the art will readily recognize that other brands of smart cards which conform to these standards and provides secure data storage functions may be substituted without departing from the present invention.”

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include a confirmation means for confirming whether setting of the second key by the first key setting means normally ends in order to allow a user to know whether or not the operations he or she chose to perform completed successfully.

However:

Mooney et al. fails to explicitly disclose an embodiment wherein **a plurality** of second keys for encoding or decoding a first key are stored in the IC card. The Applicant has further amended claim 2 to recite: *"the generated first key being encoded by said plurality of second keys in the former IC card"*. While Mooney discloses a that a plurality of keys should exist for both cards, Mooney only discloses the implementation for the transfer and encryption of one key. (Column 11, lines 1-35)

However, those of ordinary skill in the art would recognize however, that while Mooney discloses the key duplication method for a single key, such a method may be used more than once and in that sense may be applied to a plurality of keys. For example, if a document discloses how information may be transferred between one disk to another disk, those of ordinary skill in the art would determine that this process would be repeatable, thereby allowing for a plurality of information transfers, and in Mooney's case a plurality of keys.

Art Unit: 2134

However, Mooney et al. fails to disclose an embodiment wherein the plurality of second keys are stored in the former IC card. Mooney instead discloses that the origin of the second key used to encode the first key comes is derived from a question and a response and presumably discards the key after its usage. More specifically, Mooney et al. fails to disclose that a second index of key encrypting keys is stored to an IC card.

For this reason, the rejections to claim 1 are withdrawn, and claim 1 is allowable.

In reference to claim 6:

An IC card duplication method using a first IC card to be duplicated in which at least a first key for encoding or decoding data is stored, a duplicating second IC card, and a terminal unit for handling these first and second IC cards, comprising:

A first step of transmitting a key-setting instruction to which a plurality of second keys for encoding or decoding the first key is added from the terminal unit to the first and second IC cards;

A second step of receiving the key-setting instruction transmitted from the terminal unit and storing the plurality of second keys added to the key-setting instruction in the first and second IC cards;

A third step of transmitting a key takeout instruction from the terminal unit to the first IC card;

A fourth step of receiving the key takeout instruction transmitted from the terminal unit, encoded the first key by the plurality of second keys stored in the second step, and transmitting the encoded first key to terminal unit in the first IC card;

Art Unit: 2134

A fifth step of receiving the encoded first key transmitted from the first IC card and transmitting an encoding-key setting instruction to which the received encoded first key is added the second IC card in the terminal unit; and

A sixth step of receiving the encoded-key setting instruction transmitted from the terminal unit, decoding the encoded first key added to the encoding-key setting instruction by second key stored in the second step, and storing the decoded first key in the second IC card.

Claim 6 is allowable for similar reasons.

In reference to claim 6:

Mooney et al. (Column 11, lines 7-35) discloses an IC card duplication method using a first IC card to be duplicated in which at least a first key for encoding or decoding data is stored, a duplicating second IC card, and a terminal unit for handling these first and second IC cards, comprising:

- A first step of transmitting a key-setting instruction to which a second key for encoding or decoding the first key is added from the terminal unit to the first and second IC cards, where the key setting instruction is the instruction which initializes the key transfer option, and the second key is the key generated to encrypt the key that is to be transferred. (Column 11, lines 7-35)
- A third step of transmitting a key takeout instruction from the terminal unit to the first IC card, where the key takeout instruction instructs the first IC card to have its key read. (Column 11, lines 10-15)

Art Unit: 2134

- A fourth step of receiving the key takeout instruction transmitted from the terminal unit, encoding the first key by the second key stored in the second step, and transmitting the encoded first key to the terminal unit, where the first key is the key from the smartcard, the second key is the key used to encrypt the first key, and the transmission passed through the PC terminal unit. (Column 11, lines 7-35)
- A fifth step of receiving the encoded first key transmitted from the first IC card and transmitting an encoding-key setting instruction to which the received encoded first key is added to the second IC card in the terminal unit, where the encrypted or encoded first key is transmitted from the first IC card to be stored in the second unit, which is the guest smart card (Column 11, lines 7-35)
- A sixth step of receiving the encoding-key setting instruction transmitted from the terminal unit, decoding the encoded first key added to the encoding-key setting instruction by the second key stored in the second step, and storing the decoded first key in the second IC card, where key first from the user smart card is decoded or decrypted with the second key and storing the decoded key into the user smart card. (Column 11, lines 15-16)

Mooney et al. fails to explicitly disclose a second step of receiving the key-setting instruction transmitted from the terminal unit and storing the second key added to the key-setting instruction in the first and second IC cards.

Art Unit: 2134

Mooney simply discloses that this second encryption key must be sent to the user of the second card.

It is evident from Mooney et al, however, that a key may be easily store a key, whether it be an encryption key or regular key.

It would have been obvious to one of ordinary skill in the art at the time of invention to store the key for encoding and decoding in the first IC card in order to maintain greater security by having the generated encoding key remain completely confined to the smartcard thereby making the compromising of the key more difficult. (for example, the keys may now be confined to password access) (Column 3, line 67 – Column 4, line 5)

Mooney et al. however fails to disclose an embodiment where a **plurality** of second keys are stored. Specifically, Mooney et al. fails to disclose a second index of key encrypting keys or the storing of a second plurality of keys used to encrypt first keys. As opposed to the “storing” of a single key, which is virtually inherent or obvious because all keys must be at least stored in memory in order to be used. Any piece of data, including a key used to encrypt, must be stored, even if temporarily, to use manipulated in a mathematical operation or instruction. However, Applicant’s amendments call for the storing of a plurality of second keys in the IC card. No art can be found nor motivation to change can be found to call for the storing of a second index of

Art Unit: 2134

key encrypting keys used to encrypt first keys. For this reason, the rejections to claim 6 are withdrawn and claim 6 is allowable.

Claim 10 is substantially similar to claim 6 and is allowable for the same reasons.

Claims 4 and 5 are dependant upon claim 6 and are allowable for those reasons.

Conclusion

3. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

Feburary 4th, 2006